Massachusetts Department of Public Health Confidentiality Procedures

Procedure Title:	The Electronic Transmission of Confidential Information		
Procedure Number:	10-A	Version #	3.1
Effective Date:	October 1, 2007		

PART I: POLICY & DEFINITIONS

A. Policy

The Massachusetts Department of Public Health (MDPH) prohibits the electronic transmission of Confidential Information whether within the body of an Email, as an Attachment, or as a File Transfer unless the Bureau or workforce member has received a waiver from the Privacy & Data Access Office. Exemptions to this policy are named below. All other electronic transmissions require the approval of the MDPH Privacy & Data Access Office.

Due to the identity theft risk associated with their loss, the Massachusetts Department of Public Health prohibits the electronic transmission of Social Security Numbers except under extraordinary circumstances. Bureaus and programs seeking approval to transmit Social Security Numbers will be required to demonstrate that their electronic transmission is required to accomplish the business requirement.

B. Rationale

All information transmitted electronically is at risk of tampering or disclosure whether inadvertently, maliciously, or through human error. The use of encryption technology and attention to process mitigates the risk associated with the electronic transmission of information. There is additional risk of identity theft associated with the inadvertent disclosure of Social Security Numbers.

C. Purpose

This procedure describes:

1) The Department of Public Health's policy prohibiting the electronic transmission, including File Transfer, of Confidential Information;
2) The Bureaus which are exempt from this policy;
3) The framework within which an MDPH Bureau may seek a waiver from the prohibition against the electronic transmission of Confidential Information;
4) The process for the electronic transmission of Confidential Information within the state domain; and
5) The process for the electronic transmission of Confidential Information between external entities, i.e., third parties such as contractors and health care facilities.

D. Definitions

Attachment - A file that is sent with an Email message. The file can be of any type (e.g., a spreadsheet, a word processing document, or an image).

Confidential Information – For the purposes of this policy, any individually identifiable information, including, but not limited to, medical and demographic information that:

1) Reveals the identity of the subject or is readily identified with the data subject such as name, address, telephone number, social security number, health identification number, or date of birth;
2) Provides a reasonable basis to believe that the information could be used, either alone or in combination with other information, to identify a data subject;
3) Includes any protected health information as defined by HIPAA and any personal data, as defined by FIPA. See http://healthnet.dph.state.ma.us/privsec/glossary.htm#C; or
4) Includes health information or reference to an application to, enrollment or participation in any MDPH or EOHHS program.

Electronic Transmission – For the purposes of this policy, the use of Email and File Transfer protocols such as SFTP, SFED, and NDM to exchange information over a computer network

Email - A system for sending and receiving messages electronically over a computer network, as between personal computers.

File Transfer – A process used to copy a flat file from one computer to another over a computer network.

Secure File and Email Delivery System (SFED) – A system used by Commonwealth governmental agencies to ensure the security of electronic transmission of Confidential Information. The SFED system uses encryption to protect data during transmission.

Definitions (cont.)	*State Domain* – The Commonwealth of Massachusetts' wide area network (WAN). The Email system operates in this network. Email users are assigned an address ending in "state.ma.us."

PART II: EXEMPTIONS & WAIVERS

A. Exemptions

The following are exempt from the general policy prohibition against the electronic transmission of Confidential Information. Exempt Bureaus or individuals are still required to follow the protocols for sending Emails with Confidential Information outlined in Part III of this procedure.

Bureau/Individual	Circumstances
MDPH hospitals	• When emailing within or between MDPH hospitals • When emailing between a MDPH hospital and the Bureau of Public Health Hospitals • When emailing between a MDPH hospital and the MDPH Office of General Counsel; or • When emailing between a MDPH hospital and representatives of the Department of Mental Health with respect to common Clients.
MDPH Workforce Members	Between MDPH workforce members and Human Resources when using Email to conduct personnel matters.
MDPH Workforce Members	When an email is misdirected to a DPH workforce member, it may be forwarded to the appropriate DPH workforce member if the original email comes from an address outside state.ma.us and it is from the individual about whom the information relates or is from an advocate for that individual with the consent or implied consent of that individual.

All other electronic transmissions of Confidential Information require the approval of the MDPH Privacy & Data Access Office.

B. Obtaining Approval to Transmit Confidential Information Electronically

MDPH Bureaus may apply to the Privacy and Data Access Office for approval to transmit Confidential Information electronically using the "Application to Transmit Confidential Information Electronically." The application must include:

- A description of the business justification (see "Business justification" below);
- A description of the Confidential Information that the Bureau proposes to transmit electronically. This should contain only the minimum necessary data elements required to accomplish the intended purpose of the transmission. Social Security Numbers may not be included unless the Bureau or Program is required to transmit them and the business need is essential.
- The name of each state agency workforce member who will be approved to transmit the approved Confidential Information data elements;
- The name of each external user (individuals not within the state.ma.us domain) who will be approved to conduct electronic transmissions of the approved Confidential Information data elements and who will require SFED accounts (see "Protocol 2: SFED," Part IIIE); and
- The Bureau director's signature.

The signed application should be submitted to the Privacy Officer, c/o the Privacy & Data Access Office, 250 Washington Street. An electronic copy of the application should be forwarded to the Privacy Officer's attention as well.

Note: Applications for approval are transaction-specific. Additions to or modifications to approved transmissions require the submission of a new or amended application for approval. Bureaus and Programs are expected to inform the Privacy & Data Access Office of changes and additions to application contacts, state agency workforce members, and external users involved in transmitting Confidential Information.

C. Business Justification and the Application Evaluation

Applications will be evaluated by the Privacy & Data Access Office based on a review of:

a) the Bureau's business justification;
b) adherence to disclosure requirements as described in Confidentiality Procedure #3 (http://healthnet.dph.state.ma.us/privsec/downloads/procedure_03_use_disclosure.doc)
c) adherence to standards for the disclosure of the minimum amount of Confidential Information necessary to achieve the business requirement; and
d) the existence, if necessary, of any data-sharing agreements.

PART III: TRANSMITTING CONFIDENTIAL INFORMATION ELECTRONICALLY

The required procedures below apply only to Bureaus that are exempt from the policy prohibiting the electronic transmission of Confidential Information or to Bureaus that have applied for and received a waiver from this policy from the Privacy & Data Access Office.

A. Email Conventions

- Use this or similar language as a Header or Footer: "This mail [and attachment] is intended for authorized individuals and contains confidential information. If you have received this message in error and are not the intended recipient, please notify the sender."
- Do not use any Confidential Information in the subject line of the Email.
- Verify the intended recipients (the individuals included in the "TO" field) prior to sending the message. Use prepared contact lists whenever possible.

B. File Transfers

File Transfers are used to send files under two circumstances:

1) Within MAGnet (the Email ends "state.ma.us") **if** the file is too large to be sent as an Attachment

Example
The Prescription Monitoring Program Database.

Non-Example
An Excel spreadsheet containing the names of individuals who divorced in February 2003. *(This is an Attachment, not a file.)*

2) To **all** Email addresses outside of MAGnet (Email addresses not ending "state.ma.us").

C. How to Determine the Correct Protocol to Use

If you are sending …	Then Go To …
An Email or an Attachment within DPH or to another state agency (the Email ends in "state.ma.us")	Protocol One: "Confidential"
A File Transfer within DPH or to another state agency (the Email ends in "state.ma.us")	Protocol Two: "SFED"
An Email, Attachment, or a File Transfer to or from an external organization	Protocol Two: "SFED"

D. Protocol One: "Confidential Email"

Type "Confidential" in the subject line of the Email to be sent. It is not case-sensitive and does not need to be boldfaced.

E. Protocol Two: "SFED"

1. Request an SFED account from the MDPH Help Desk.
2. Click on the link below to be connected to the "Secure File and Email Delivery System" user manual:

Note: EOHHS agency users will be assigned a special SFED account that will end "eohhs-sfed.state.ma.us."

Example: emily.publichealth@eohhs-sfed.state.ma.us

SFED users should be sure to direct all their SFED incoming and outgoing Email to their SFED accounts and not to their regular work Email (i.e., the account ending "state.ma.us").

Important Note: SFED users may not open SFED incoming Email in public areas on Personal Digital Assistants (e.g., blackberries) or laptop computers.

PART IV: ADMINISTRATIVE REQUIREMENTS

A. Training Requirements

It is the responsibility of each MDPH Bureau to ensure that each workforce member completes the training prior to transmitting Emails containing Confidential Information. Completion of the training must be documented. It is also the responsibility of the approved Bureau to train any individuals (either state agency workforce members or external users) who will be using SFED (either as a sender or as a receiver) in this application.

This requirement applies to both exempt Bureaus and Programs and those who are approved to email Confidential Information by means of a waiver.

If you will be using	You must take the on-line training located at
Protocol One: Confidential	http://healthnet.dph.state.ma.us/privsec/training/email/email01.htm).
Protocol Two: SFED	http://healthnet.dph.state.ma.us/privsec/training.htm

B. Self-Audit Requirements

Bureaus receiving a waiver authorizing them to transmit individual-level Confidential Information electronically must conduct an annual self-audit to ensure that:

1. The list of approved workforce members is current;
2. All approved workforce members have completed training;
3. Only the minimum necessary Confidential Information is being sent;
4. The electronic transmission of Confidential Information is used only for the purpose(s) identified in the original application;
5. Appropriate headers or footers are included in the Emails and/or File Transfers;
6. Confidential Information is not written in the subject line of the Emails;
7. The word, "Confidential" is typed in the subject line of the Emails;
8. Prepared contact lists are used whenever possible; and
9. Emails are appropriately saved.

A copy of this self-audit may be requested by the Privacy & Data Access Office.

C. Record Retention

In accordance with the Public Records Law, all substantive Emails must be preserved. While portions of any Emails sent pursuant to this procedure are likely exempt from disclosure because they contain Confidential Information identifying an individual, they still must be saved pursuant to the statewide Retention Schedule. The Bureau should either print a copy for inclusion in the individual's file or save the message in an Outlook archive file backed up to network storage. Email containing Confidential Information may only be saved on MDPH-owned computers unless the computer is otherwise approved by IT Services for use with MDPH Confidential Information. Emails containing Confidential Information should not remain in the workforce member's inbox.

D. Security Incidents

Any privacy or security incidents, including unauthorized transmissions, should be immediately reported to the reporting workforce member's supervisor (see Procedure #2, Breaches of Confidential Information) and the Help Desk.